IN THE UNITED STATES DISTRICT COURT
FOR NORTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF: 432 Stadium Drive, Fostoria, Ohio 44830	Case No. 3:20MJ5371

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Special Agent Deane Jengelley, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 432 Stadium Drive, Fostoria, Ohio 44830, hereinafter "**Target Premises**," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent (SA) with the U.S. Drug Enforcement Administration (DEA), and have served in this capacity since graduating from the basic agent training program at the DEA Academy in Quantico, Virginia in October 2017. In January 2018 I was assigned to the Toledo Resident Office located in the Northern District of Ohio. Prior to my position with the DEA, I was employed with the Atlanta Police Department as a Police Officer from October 2013 to April 2017. While employed with the Atlanta Police Department I was a member of the Crime Suppression Team and the Criminal Investigations Division Burglary Unit.

3. As a Special Agent with the DEA, I am an "investigative or law enforcement officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer

of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516(1).

4. I am currently assigned to the Toledo Resident Office, within the Detroit Field Division of the DEA, where I participate in investigations targeting individuals and organizations involved in drug trafficking offenses in the Northern District of Ohio and elsewhere. At all times during the investigation described herein, I am acting in an official capacity as a Special Agent with the DEA.

5. I have received specialized training at the DEA Training Academy in Quantico, Virginia, regarding the identification of narcotic controlled substances and the operation of drug trafficking organizations. I have also been involved in the investigation of numerous individuals and organizations involved in the distribution and use of controlled substances. During my employment with the DEA as a Special Agent, I have participated in many aspects of drug investigations including conducting physical and electronic surveillance, phone toll analysis, collection of electronic evidence, working as an undercover, executing arrests, interviews of admitted drug traffickers, drug users and informants. I have prepared affidavits in support of numerous search warrants for violations of federal drug laws contained in Title 21, United States Code, and have executed the same.

6. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

7. On November 23, 2020, while reviewing postal business records, Postal Inspectors identified a U. S. Postal Service Priority Mail Express parcel bearing tracking no. 9405 5118 9956 4113 6971 57, addressed to James Rodriguez, 914 Spruce St, Fostoria, OH 44830 (hereinafter "**Original Target Premises**") bearing a return address of Mark Rodriguez, 1931 Majella St, Edinburg, TX 78542

(hereinafter "**Subject Parcel**") as a suspected drug parcel based on several factors including but not limited to origin, method of mailing, and size.

8. The **Subject Parcel** is further described as a U.S. Postal Service Priority mail flat rate shipping box, weighing approximately 5 pounds and 13 ounces. The **Subject Parcel** was mailed on November 23, 2020 from a contract postal unit (CPU) in Mission, Texas 78572.

9. Postal inspectors made inquiries through an open source database, and were not able to associate the name James Rodriguez to 914 Spruce Street, Fostoria, Ohio 44830 nor Mark Rodriguez to 1931 Majella Street, Edinburg, Texas 785452. Your affiant knows based on his training and experience, individuals using the U.S. mail for the purpose of transporting controlled substances will often place fictitious address and/or name information on packages to conceal their true identities from law enforcement should the parcel be seized.

10. On November 30, 2020, the **Subject Parcel** was subjected to "Ciga", a narcotic detection canine handled by Detective Twombly of the Cuyahoga County Sheriff's Department, at the U.S. Postal Inspection Service Cleveland Field Office in a parcel line-up, which contained parcels that do not contain any narcotics. Ciga gave a positive alert on the **Subject Parcel**. According to Detective Twombly, this positive alert meant Ciga detected the odor of an illegal drug emanating from the parcel.

11. Detective Twombly has been State Certified as a Narcotics Canine handler and he and narcotics canine Ciga have worked together since 2013. Detective Twombly and canine Ciga were both certified in November 2020 by the Ohio Peace Officers Training Academy (OPOTA) and the North American Police Work Dog Association (NAPWDA) in December 2019. Detective Twombly and canine Ciga have both completed 80 hours of a state-certified training program at Shallow Creek Kennels in Sharpsville, Pennsylvania under Certified Trainer John Brannon of the NAAPWDA, a nationally organized police work dog association that provides training for dogs and handlers. During this time, Ciga was

trained and certified to alert to the presence of the odors of marijuana, cocaine, heroin, MDEA (methlyenedioxyethlamphamine), methamphetamine ("crystal meth"), and/or their derivatives. Detective Twombly has been trained how to handle a detector K-9 and read his alerts. According to Detective Twombly, Ciga is a reliable K-9 assist unit.

12. On November 30, 2020, Postal Inspector Brandon Holestine authored an affidavit in support of a search warrant for the **Subject Parcel**. On November 30, 2020, United States Magistrate Judge Thomas M. Parker reviewed and signed the search warrant.

13. The search warrant was executed, and a search of the **Subject Parcel** revealed two (2) rectangular shaped objects wrapped in foil, black tape, and clear plastic, weighing approximately 2.165 kilograms. Postal Inspector Brandon Holestine opened both objects and identified a white powdery substance that was pressed into the shape of a rectangle. Postal Inspector Brandon Holestine conducted a standardized field test on the white powdery substance, and it produced positive results for Cocaine.

14. Database records indicate that the **Subject Parcel**'s USPS tracking information was actively monitored during its transit via a mobile data connection, as follows:

Source IP/Phone/Email	Date	Time (Central)	Domain/ISP
2607:fb90:e613:a416:70ae:295b:3c4:bb76	11/27/2020	03:33:08	T-MOBILE USA INC.
2607:fb90:e613:a416:70ae:295b:3c4:bb76	11/27/2020	13:59:21	T-MOBILE USA INC.
2607:fb90:c293:e14a:867:56de:f7bf:8cc3	11/27/2020	09:41:42	T-MOBILE USA INC.
2607:fb90:c293:e14a:867:56de:f7bf:8cc3	11/28/2020	08:29:00	T-MOBILE USA INC.

15. On November 30, 2020, your Affiant authored an affidavit in support of an anticipatory search warrant to search the **Original Target Premises**. That same day, the Honorable Magistrate Judge Carmen E. Henderson reviewed and signed the search warrant.

16. On December 1, 2020, a controlled delivery of the **Subject Parcel**, with the cocaine removed and replaced with sham, was attempted at the **Original Target Premises**. After the **Subject Parcel** was dropped on the front step of the **Original Target Premises**, a blue Chevy Suburban bearing Ohio Registration GMX 1535 arrived at the **Original Target Premises**. A Hispanic male, later identified as Roman FLORES, exited the blue Chevrolet and SA Noel observed FLORES pick up the **Subject Parcel** and carry it back to the blue Chevrolet. SA Noel observed FLORES enter the blue Chevrolet with the **Subject Parcel** and back out of the driveway.

17. TFO Brotherton and SA Jengelley then observed FLORES begin traveling southbound on Spruce Street. Surveillance units conducted physical surveillance on the FLORES and the blue Chevrolet until FLORES parked on Stadium Street, in front of the **Target Premises**, 432 Stadium Street, Fostoria, Ohio. TFO Brotherton and SA Jengelley observed FLORES exit the blue Chevrolet with the package in his left hand. TFO Brotherton and SA Jengelley observed FLORES walking through the yard/sidewalk towards the **Target Premises**. SA Noel then observed FLORES open the glass screen door. SA Noel then observed FLORES standing in the doorway.

18. FLORES was looking all around and it was apparent that he was looking for law enforcement, based on investigators' training, knowledge and experience. Surveillance units could not sit stationary in front of the **Target Premises** so continuous drive-bys were conducted. SA Noel then observed the door closed and no longer observed FLORES. SA Noel then observed FLORES and another Hispanic male, later identified as Matthew REZA standing outside of the residence. SA Noel then observed REZA next to the black GMC Terrain.

19. Based on these observations, SA Noel had his visible red/blue lights activated and REZA began walking away from the GMC. FLORES was no longer outside and was back inside the residence.

20. Investigators approached the **Target Premises** with full Police markings and visible red/blue lights. Entry was made to the residence as SA Noel placed REZA under investigative detention. Investigators cleared the residence and TFO Brotherton located FLORES in the bathroom, with the sink water running. Investigators placed FLORES under investigative detention. In plain view, Investigators observed a digital scale, a red cup and a spoon in the sink, underneath the running faucet. Investigators also observed a freezer bag with a white powder like residue on the bag (suspected cocaine) also a white chunk of the same substance (suspected cocaine) was observed in the bottom of the toilet.

21. The Subject Parcel was observed inside the black GMC Terrain, opened, with what appeared to be just one kilogram of sham missing. Investigators believe that the missing kilogram of sham is still inside the **Target Premises**.

22. An electronic video surveillance system was observed on the front porch of the **Target Premises.** In my law enforcement experience, these electronic video surveillance systems often are connected to physical recording devices, such as hard drives, inside a residence.

23. At the time of his detention, FLORES possessed a black iPhone and a black Motorola cell phone. The iPhone was in FLORES' hand as he attempted to put a cocaine-like substance in the toilet, and the black Motorola cell phone was on the floor near the toilet and ringing with a call from a 956- area code Texas number.

24. A black Samsung phone was in REZA's pocket when we was detained in the driveway near the **Subject Parcel**.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

25. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

26. *Probable cause.* I submit that if a computer or storage medium (hereinafter "computer") is found on the **Target Premises**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

27. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **Target Premises** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record

additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses

through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

28. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

30. Because several people may share the **Target Premises** as a residence, it is possible that the **Target Premises** will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

31. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

32. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned

that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Deane Jengelley

Deane Jengelley
Special Agent
Drug Enforcement Administration

Sworn to via telephone on this 1st day of December, 2020,
after submission by reliable electronic means.
Fed.R.Crim.P. 4.1 and 41(d)(3).

Carmen Henderson

CARMEN E. HENDERSON
UNITED STATES MAGISTRATE JUDGE